

**REMARKS**

In view of the foregoing amendments and following remarks, Applicant respectfully requests favorable reconsideration of the application.

Applicant respectfully thanks the Examiner and her supervising Examiner for the kind and courteous telephone interviews granted and conducted on October 18 and 19, 2005 in connection with this application, in which the Office identified and clarified at least one key issue with respect to the pending claims that, presumably, will now lead to the allowance of this application.

Claims 1-33 are pending in this application. In the Final Office Action issued prior to the filing of the accompanying Request for Continued Examination, the Office had rejected all claims under 35 U.S.C. §103 as being unpatentable over Howard in view of Othmer.

**The Present Invention**

The present invention comprises a method for synchronizing a particular computer user's cookies across a plurality of computers that the single user may use to access the Internet. Particularly, it is not uncommon for a single person to have multiple computers that he or she uses on a regular basis for accessing the Web. It is therefore likely that all of those computers will not simultaneously have the most current cookies for that user.

Thus, in accordance with the present invention, a user with multiple computers registers with a service that will synchronize cookies across all of the user's computers. More particularly, a server is maintained on a network such as the World Wide Web for

storing cookies and/or cookie change information for a user that registers with the service (hereinafter termed the Cookie Synchronization Server). Each user opens an account and registers all of his or her computers under that account. Each of these computers is equipped with software that monitors all changes made to cookies at that machine and sends a notification to the Cookie Synchronization Server including sufficient information to at least (1) identify the account to which the client belongs; and (2) allow the cookie synchronization server to recreate the cookie. In a preferred embodiment, the computer simply sends the entire cookie and an account ID with the request.

The Cookie Synchronization Server stores the information and subsequently sends it out to each other client machine registered under that account. The server may, for instance, send out the information to the registered client machines responsive to receipt of requests for the information from the other client machines. The client machines update their cookies accordingly and send an acknowledgement receipt to the Cookie Synchronization Server. Thus, the Cookie Synchronization Server can keep track of which client machines have the latest version of each cookie so that it can send only those cookies that the client machine does not already have to a requesting client machine.

#### **The Howard Reference**

The Howard reference pertains to a technique for simplifying for a computer user the accessing of web sites that require a user to register to access the website.

Typically, the registration process comprises entering a previously designated user ID and/or password.

Figure 4 is most illustrative of the teachings of the Howard reference that the Office deems relevant to the present invention. In accordance with Howard, a plurality of web sites register to be part of this particular service. The servers operated by those web sites are termed "affiliate servers". In addition, the provider of the invention provides another server on the Web termed the "authentication server". When a user accesses a web site that requires authentication (i.e., entry of a user ID and/or password), the affiliate server passes the client request on to the authentication server instead of servicing it itself. The authentication server sends the client machine a sign-in page. When the user enters the proper password and/or user ID, the authentication server copies the appropriate cookies to the client machine and redirects the user's browser back to the affiliate server. The authentication server also generates an authentication ticket and transmits it to the affiliate server informing the affiliate server that the user has been properly authenticated. The authentication server also communicates the user profile information to the affiliate server through the client machines.

The reference has nothing to do with maintaining cookie consistency across a plurality of client machines.

#### **The Othmer Reference**

Othmer discloses a technique for remotely monitoring a plurality of networked computers for purposes such as beta testing of software. With specific reference to

Figure 1 of Othmer, the computers 34, 36, 38, and 40 that are being monitored are equipped with a nub 42 (e.g., a software application) that gathers information about the operation of a software application being executed by the associated computer or about the operation of the microprocessor. The information gathered by the nub is collected into a "black box" data structure 44 that is transmitted over the network to a centralized server 32 that collects and analyzes the data from the various computers 34-40.

The portion of Othmer on which the Office relies discloses that the central server 32 may transmit customized configuration data 46 in a configuration file to each computer 34-40 so that each nub 42 in each computer 34-40 may be customized so that the information gathered by each nub may be selectively specified.

#### **Discussion of Prior Art Rejection**

Taking independent claim 1 as an example, the Office asserted that Howard teaches the invention as claimed including a method of synchronizing cookies across a plurality of computing devices that access a network, the method comprising the steps of: (1) registering the plurality of computing devices as members of an account (column 2, lines 1-42 and column 5, lines 42-67); (2) maintaining information as to the members of the account at a server (column 10, line 55 through column 11, line 15); (3) responsive to a change in one or more cookies stored at a first one of said computing devices, that computer device sending a message to a server containing sufficient data from which said one or more cookies can be determined and the account number (column 7, lines 1-15); (4) storing at the server the data and information identifying the account (column 8, line 32 through column 9, line 65); and (6) the other member

computing devices updating their cookies in accordance with the data received from the server (column 7, lines 25-39).

The Office concedes that Howard does not explicitly teach the server sending the data to the other members of the account. However, the Office cites Othmer as teaching a server sending data to other members of an account (column 5, line 40 to column 6, line 25).

The Office asserted that it would have been obvious to implement the teachings of Othmer into the computer system of Howard to have the server sending data to other members of the account because it would have an efficient system that could provide specific functions that simultaneously send the same message to multiple recipients.

Applicant respectfully traverses. There are at least two flaws in the Office's analysis. First and foremost, Howard does not teach anything even remotely resembling the present invention, let alone something that meets the five claim elements asserted by the Office. Secondly, there is absolutely nothing in the prior art that suggests the proposed combination of Howard and Othmer.

Turning first to the teachings of Howard, Howard has absolutely nothing to do with synchronizing cookies across a plurality of computers. Step 1 of claim 1 recites "registering a plurality of computing devices as members of an account." The Office refers to column 2, lines 1-42 and column 5, lines 42-67 as teaching this limitation. However, these portions of Howard merely teach that a plurality of affiliate servers and a plurality of client machines register with the server. There are no separate accounts in the service. Rather, you either are a subscriber to the service or you are not a

subscriber to the service. Individual users do not have separate accounts with the service.

Nevertheless, even if we assume, for the sake of argument, that the language of step 1 of claim 1 is broad enough to read on this aspect of Howard, step 3 of claim 1 recites “responsive to a change in one or more cookies stored at a first one of said computing devices that is a member of said account, said first member computing device sending a message to a server on said network containing sufficient data from which said changes to said one or more cookies can be determined and the account to which said first member computing device corresponds.” The Office cites column 7, lines 1-15 as teaching this limitation.

Column 7, lines 1-15 of Howard are reproduced below for ease of reference.

Upon receiving the information from the user of the client computer system, the authentication server compares the entered information with the information stored in the authentication database (step 208). If the user-entered information is not correct (i.e., does not match the information stored in the authentication database) then the authentication server generates and communicates a web page to the user indicating the login ID and password combination were not valid (step 210). The web page may give the user an opportunity to re-enter the login ID and password by returning to step 204. Confidential information (such as the login ID and password) is communicated using a secure protocol such as SSL (secure sockets layer). Various other secure protocols or encryption mechanisms can be used to communicate confidential information between the authentication server and the client computer system.

This portion of Howard describes how the authentication server, responsive to the user inputting the requested user ID and password, checks if they are correct. This simply has nothing whatsoever to do with step 3 of claim 1. Nothing is done in response to a change in any cookie, as claimed in claim 1. No account number

corresponding to a plurality of computing devices is sent from the client to the server, as claimed in claim 1.

In response to Applicant's previous arguments that Howard does not teach synchronizing cookies across a plurality of machines, the Office argues that, in Howard, teaches that "the cookie is updated adding the current affiliate server to the list of sites visited", referring to column 7, lines 30-39, which recite:

The cookie is updated by adding the current affiliate server to the list of sites visited. This list of sites visited is used to remove cookies from the client computer system when the user logs out of the authentication server. For example, when the user logs out, the authentication server sends a message to each web server on the list of sites visited. Each message is a request for the web server to delete any cookies it placed on the client computer system (e.g., through a browser running on the client computer system).

This section of Howard merely discloses updating a cookie at the single client machine. Certainly Applicant concedes that updating cookies is known in the prior art. In fact, that is the basis of the present invention. Specifically, since (1) cookies do, in fact, often get updated at one client machine and (2) individuals often access the Web using multiple client machines, there is a need for an invention like the present invention that synchronizes cookies across the multiple machines of a single individual. The fact that Howard teaches updating a cookie at a single client machine is not the invention. It is the problem solved by the present invention.

*On October 19, 2005, the supervising Examiner identified an issue with the claims that Applicant had not previously appreciated and that appears to be the key basis of the present prior art rejections. Applicant has now addressed that issue in the amendments above and comments below, such that the all of the claim rejections*

*should now be overcome. Applicant respectfully thanks the supervising Examiner for her guidance on this matter. Particularly, the supervising Examiner noted that the wording of step (3) of claim 1 did not recite that the changes to the one or more cookies were communicated to the server, but merely that "said one or more cookies" were communicated to the server. The supervising Examiner pointed out that this language could read on the old cookies, not the changed cookies. Furthermore, as a result of the same language in the original claim 1, it was very vague as to what data was being sent to the other members of the account, such that the claim language could be read extremely broadly on all sorts of data sent between two computer nodes on a network.*

*The amendment to claim 1 hereinabove clarifies this claim language and clearly prevents any possible reading of claim 1 onto the combination of Howard and Othmer. Specifically, step (3) of claim 1 now clearly recites that it is the changed cookie information that is being sent in step (3) (as well as step (5)).*

Howard, having nothing whatsoever to do with synchronizing cookies across a multiplicity of client machines, is essentially irrelevant to the present invention.

Accordingly, the rejection of claim 1 based on the combination of Howard and Othmer should be withdrawn since Howard clearly does not disclose step (3) of claim 1.

In addition, the Office has already conceded that step (5), i.e., the step of sending the changed cookie data to the other members of the account, is not found in Howard. This, of course, is true as there are no accounts in Howard and no changed cookie data is sent to other clients.



However, the Office has cited Othmer as teaching this claim element and asserted that it is obvious to combine this aspect of Othmer with the system of Howard. However, nothing could be further from the truth. First, the above-mentioned amendment to step (3) carries over to step (5), which refers to the same “data” mentioned in step (3). Thus, step (5) now recites that it is the changed cookie data that is being sent in step (5).

Secondly, Othmer is essentially irrelevant in any event. Specifically, Othmer discloses a technique for sending system information from a plurality of computers to a central server so that the central server can collect and evaluate that information. According to the Office, as part of that technique, the central server in Othmer sends data to the plurality of computers and this corresponds to element 5 of claim 1.

Like Howard, Othmer has absolutely nothing to do with synchronizing cookies across a plurality of client machines. Accordingly, Othmer’s relevance is that it teaches a server that sends a piece of information to more than one client machine. Applicant certainly concedes that this has been done in the prior art. However, its relevance to the present invention is specious at best.

As set forth in MPEP §2143, a proper obviousness rejection has three basic requirements:

First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art to modify the reference or to combine the reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

We have already shown that the third requirement is not met as Howard does not teach that for which it has been cited. However, the proposed combination also fails to meet the first requirement, i.e., that there be some suggestion in the art for the proposed combination. The Office asserts that it would have been obvious to combine Howard and Othmer in order “to have a server sending data to other members of the account because it would have an efficient system that can provide specific functions that simultaneously send the same message to multiple recipients”.

This alleged justification makes no sense. First of all, Othmer does not send cookie data to other client machines, let alone changed cookie data. It sends configuration data. The word “cookie” does not appear in Othmer. Thus, Othmer does not even teach that for which it has been cited, and therefore, the rejection fails the third requirement of a proper obviousness rejection for this additional reason.

Secondly, there is no suggestion to combine. In Howard, there is no information that it would make sense to send to other computers. In fact, there are no relevant “other computers” in Howard. There is the affiliate server, the authentication server, and the client machine. The authentication server sends a cookie to the client machine and sends an authentication ticket to the affiliate server. There is absolutely no reason to send Howard's cookie (or any other cookie, for that matter) to any other machine.

Thus, the mere existence of a reference such as Othmer that discloses sending data from a server to a plurality of client machines disembodied from any teaching in the prior art as to why one would want to do that in connection with changed cookies cannot possibly lead one to the present invention.

The Office asserts that it is obvious to have a server send data to other members of an account because it is efficient to provide specific functions to multiple recipients. However, in Howard, there is no need to do that. It has nothing to do with the purpose or function of Howard.

The Office has done nothing more than attempt to find the individual element of step (5) of claim 1 in a secondary reference having no connection whatsoever with the primary reference (or the present invention). Moreover, the Office has not even found a reference that teaches step (5) because Othmer does not disclose a "server sending said data to other members of said associated account" (claim 1, step (5)), wherein that "data" is "data from which said changes to said one or more cookies can be determined" (claim 1, step (3)). Othmer sends configuration data in a configuration file about a program that is being beta tested (column 5, line 40 to column 6, line 25).

Quite simply, there is absolutely no support for the conclusion that a skilled artisan looking at a first reference that deals with a simplified method for registering a client machine at multiple web sites (Howard) and a secondary reference dealing with retrieving computer system information for purposes such as beta testing of new software (Othmer), suggests any technique whatsoever for

synchronizing cookies across a plurality of client machines, let alone a technique meeting the limitations of claim 1.

Claims 2-15 depend from claim 1 and, therefore, distinguish over the prior art of record for at least all of the same reasons as claim 1.

Independent claim 16 is similar to claim 1 and therefore distinguishes over the prior art of record for at least all of the same reasons as claim 1. Particularly, claim 16 is similar to claim 1, the major difference being that claim 16 is written specifically from the perspective of the server and, therefore, recites acts performed by the server, whereas claim 1 is a system claim reciting acts performed at both the client machine and the Cookie Synchronization Server. Specifically, claim 16 recites “receiving messages from said computing devices that are members of said account identifying one or more cookies that have been changed at said computing devices, said messages also containing sufficient data from which said changes to said one or more cookies can be determined and the account to which first said member computing device corresponds”. It also recites “said server sending data to other computing devices that are members of said account”. These are quite similar to the limitations discussed above in connection with claim 1 that are not met by the proposed combination.

Claims 17 through 23 depend from claim 16 and, therefore, distinguish over the prior art of record for at least all of the reasons discussed above in connection with claim 1.

Independent claim 24, of course, also pertains to the same general invention as claims 1 and 16. Claim 24, however, is written from the perspective of one of the client machines that is a member of the account. The Office concedes that step 3 of claim 24, i.e., "said member computing devices receiving said data from a server on said network" is not found in Howard but, relies on Othmer for this teaching. However, as already discussed above in connection with claim 1, that proposed combination clearly is improper as there is no suggestion to make the proposed combination.

Further, the Office relies on column 7, lines 1-15 of Howard as teaching step 2 of claim 24, i.e., "responsive to a change in one or more cookies stored at any of said computing devices that are members of said account, said computing device sending a message to a server on said network containing sufficient data from which said changes to said one or more cookies can be determined and the account to which said first member computing device corresponds".

As previously discussed, column 7, lines 1-15 simply discusses the fact that the authentication server compares the user ID and/or password data input by the user with its database information to determine whether the user has input the correct ID and/or password. This has nothing to do with the recited step of sending a message to the server containing cookie and/or account information. Furthermore, it certainly is not performed "responsive to a change in one of the cookies." Accordingly, it is utterly irrelevant to step 2 of claim 24.

Claims 25-32 depend from claim 24 and therefore distinguish over the prior art for at least all of the reasons set forth in connection with claim 24.

Even further, the dependent claims further distinguish over the prior art of record. The further distinctions are numerous and will not be fully discussed since all of the dependent claims already clearly distinguish over the prior art by virtue of their dependence on the independent claims discussed above. Nevertheless, by way of example, claim 2, for instance, recites that step (5) "is performed responsive to a request for said one or more changed cookies received from another computing device that is a member of said account" and "(7) said member computing devices issuing requests for changed cookies". In Section 6 of the Office Action, the Office asserted that Howard teaches these limitations. However, in connection with claim 1, the Office has already conceded that Howard does not teach step (5). Accordingly, it could not possibly teach the further limitations restricting step (5) as recited in claim 2.

Furthermore, step (7) essentially is an adjunct to step (5). Thus, it is not seen how it is possible that Howard could teach the elements of step (7) when the Office has already conceded that Howard does not teach step (5). The same is true for claims 4-7. These claims fill in details of step (5). The Office says that these details are taught in Howard. However, the Office has already admitted that Howard does not teach step (5). Therefore, it could not possibly teach the details of step (5).

Claims 13 and 31 add the limitation that step (3) is performed further responsive to an instruction received by said member computer device to log off of said network. The Office has asserted that this is disclosed in column 8, lines 1-32 and column 6, lines 1-27 of Howard. However, Applicant has reviewed these sections of Howard and they do not appear to contain any relevant disclosure whatsoever other than the fact

that the term "logging out" or "logged out" appears in those sections utterly disembodied from any relevant disclosure.

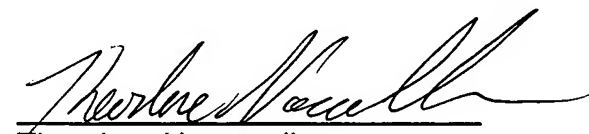
Accordingly, applicant respectfully requests the Office to withdraw the rejections of claims 1-33 in view of Howard and Othmer.

**Conclusion**

In view of the foregoing, this application is now in condition for allowance. Applicant respectfully requests the Office to issue a Notice of Allowance at the earliest possible date. The Examiner is invited to contact Applicant's undersigned counsel by telephone call in order to further the prosecution of this case in any way.

Respectfully submitted,

Dated: November 9, 2005

  
Theodore Naccarella  
Reg. No. 33,023

Synnestvedt & Lechner LLP  
2600 Aramark Tower  
1101 Market Street  
Philadelphia, PA 19107-2950  
Telephone: (215) 923-4466  
Facsimile: (215) 923-2189  
Attorneys for Applicant

TXN:pmf

M:\TNaccarella\CLIENTS\IBM\25025\Patent Office\Preliminary AMN with RCE.doc